R E M A R K S

Reconsideration of this application is respectfully requested.

According to the present invention as recited in independent claims 7, 8, 13 and 20, a portion of compressed data is extracted as encryption key data, and the compressed data is encrypted by changing the portion of the compressed data extracted as the encryption key data.

Further, according to the present invention as recited in independent claim 7, the encrypted data is decoded back to the compressed data by combining the encryption key data and the encrypted data, both of which have been generated from the same compressed data.

Still further, according to the present invention as recited in independent claims 8 and 20, the encryption key data and the encrypted data are stored, and management information showing correspondence between the encryption key data and the encrypted data, both of which have been acquired from the same compressed data is also stored. In addition, as recited in independent claims 8 and 20, the stored encryption key data and the stored encrypted data, both of which have been acquired from the same compressed data are extracted based on the stored management information, and then the extracted encryption key data and the

extracted encrypted data are combined and decoded back to the compressed data.

Yet still further, according to the present invention as recited in independent claim 13, the encryption key data and specific information which identifies the stored encrypted data corresponding to the encryption key data is output in a predetermined form to an external user.

With the structure of the present invention as recited in the independent claims 7, 8, 13 and 20, high-volume image data (for example, page data) is compressed and a portion of the compressed image data is extracted as encryption key data. In addition, the portion of the compressed image data which corresponds to the encryption key data is changed (for example, replaced with other data, deleted, etc.) And just by changing the portion of the compressed image data which corresponds to the encryption key data, according to the claimed present invention, the compressed image data becomes “encrypted” since the compressed image data with the changed portion cannot be decompressed unless the change to the compressed image data is undone. Accordingly, with this structure of the claimed present invention, it becomes impossible to decompress the compressed image data without the corresponding encryption key data. As a result, an advantageous effect of preventing unauthorized reproduction of the original image data from the compressed image

data in a simple manner is produced. See the disclosure in the specification at, for example, page 11, lines 14-17.

In the Final Office Action, the Examiner has again rejected claims 7-19 under 35 USC 102 as being anticipated by previously cited USP 7,155,012 ("Candelore et al"), and the Examiner has again rejected claim 20 under 35 USC 103 as being obvious over Candelore et al.

However, it is again respectfully submitted that Candelore et al does not disclose, teach or suggest the above described features and the advantageous effect of the present invention as recited in the independent claims 7, 8, 13 and 20.

As recognized by the Examiner on page 2 of the Final Office Action, "encryption key data" as recited in the claimed present invention is not aligned with the typical use of the term as known to one of ordinary skill in the art. However, it is respectfully pointed out that the written description clearly redefines "encryption key data" as simply being a portion of the compressed data (see, for example, Fig. 1 and page 13, lines 15-20). Indeed, encryption in the claimed present invention is clearly redefined (or defined) in the specification as being performed simply by changing a portion of the compressed data (thereby corrupting the compressed data) and by utilizing a property of the compressed data whereby even if a portion of the compressed data is changed, it <u>cannot</u> be decompressed (that is,

it becomes “encrypted”). See, for example, Fig. 1 and the disclosure in the specification at page 3, line 13 to page 4, line 3.

With respect to the cited prior art, Candelore et al discloses a mechanism for scrambling contents of a cable television or satellite broadcasting signal by, for example, encrypting data corresponding to stripes or a mosaic in an image of the broadcasting signal, in order to inhibit unauthorized use of content by subscribers. In Candelore et al, specific packet data from a video signal such a luminance, chroma or audio signal is selected, and then the selected packet data is encrypted.

More specifically, Candelore et al discloses at column 6, lines 14-20 that:

> The data are then passed along to an encrypter 154 that, based upon the PID of the packets encrypts certain packets (in accord with the present invention, these packets are the special packets which are mapped by the PID Remapper 130 to the original PID of the incoming data stream for the current program). The remaining packets are unencrypted.

Thus, the encryption in Candelore et al is, at best, merely according to the typical use of the term as known to one of ordinary skill in the art. In other words, the encryption in Candelore et al is not performed by simply changing a portion of compressed data so as to corrupt the compressed data as according to the claimed present invention. And therefore, it is respectfully submitted that Candelore et al does <u>not</u> at all

disclose or suggest the extraction and the encryption as according to the present invention as recited in independent claims 7, 8, 13 and 20 whereby a portion of the compressed data is extracted as encryption key data, and the compressed data is encrypted by changing the portion of the compressed data extracted as the encryption key data.

It is respectfully pointed out that, during examination, the USPTO must give words of a claim their plain meaning unless such meaning is inconsistent with the specification. MPEP 2111.01 I. In this case, the "encryption key data" and more generally, the encryption is clearly redefined (as allowed by MPEP 2111.01 IV) in the specification of the present application and it is respectfully submitted that Candelore et al does not disclose or suggest the encryption as according to the claimed present invention in light of the intended meaning thereof as evidenced by the disclosure in the specification and drawings.

On page 3 of the Final Office Action, the Examiner asserts that the PID of Candelore et al corresponds to the "encryption key data" as according to the claimed present invention, and the corresponding encrypted packet based on the PID of Candelore et al corresponds to the "encrypted data" as according to the claimed present invention. Applicant respectfully disagrees.

The PID of Candelore et al merely corresponds to a packet identifier which is for identifying a data packet and which is

read from the header of the data packet. In Candelore et al, based on the PID of a packet, the packet may be encrypted or left unencrypted (See column 6, lines 15-20). However, the PID of Candelore et al is not combined with the encrypted packet identified by the PID in order to decrypt the identified packet. That is, contrary to the claimed present invention, in Candelore et al, the PID of a given data packet is not extracted from the packet and the portion corresponding to the PID in the data packet is not changed in order to encrypt the data packet. Further, contrary to the claimed present invention, in Candelore et al, the PID and the corresponding encrypted packet identified by the PID are not combined in order to decrypt the encrypted packet. Therefore, it is respectfully submitted that the PID of Candelore et al does not correspond to the "encryption key data" as according to the claimed present invention, and that the corresponding encrypted packet based on the PID of Candelore et al does not correspond to the "encrypted data" as according to the claimed present invention.

Still further, according to the claimed present invention, the encryption key data and the encrypted data both of which have been generated from the same compressed data are combined and decoded back to the compressed data. That is, with the structure of the claimed present invention, simply by undoing the change to

the compressed image data, the encrypted image data is decoded back to the compressed image data.

By contrast, Candelore et al discloses at column 12, lines 8-13 that:

> When a program is received that contains encrypted content that was encrypted by any of the above techniques, the demultiplexer directs encrypted packets containing encrypted content and secondary PIDS to a secondary CA decrypter 308. These packets are then decrypted at 308 and passed to a PID remapper 312.

Thus, the decryption (or decoding) in Candelore et al is, at best, merely according to the typical use of the term as known to one of ordinary skill in the art. In other words, decryption (or decoding) in Candelore et al is not performed simply by undoing the change to the compressed image data.

Accordingly, it is respectfully submitted that Candelore et al does not disclose or suggest the decoding as according to the present invention as recited in independent claim 7 whereby the encrypted data is decoded back to the compressed data by combining the encryption key data and the encrypted data, both of which have been generated from the same compressed data.

More generally, it is respectfully submitted that Candelore et al does not disclose or suggest the decryption (or decoding) as according to the claimed present invention in light of the indented meaning thereof as evidenced by the disclosure in the specification and drawings.

Still further, on pages 3 and 4 of the Final Office Action, the Examiner asserts that Candelore et al discloses providing management information within the PSI, which identifies these selected PIDs, wherein the PSI is appended to the encoded data flow to be decoded by a separate party. Hence, according to the Examiner, Candelore et al discloses the features of the present invention as recited in independent claims 8, 13 and 20. Applicant respectfully disagrees.

Candelore et al discloses modifying Program Specific Information (PSI) after remapping. However, Candelore et al does not disclose or suggest that for a given encrypted packet, management information is provided within the PSI so as to show a correspondence between the encrypted packet and the PID thereof. In fact, since the PID itself is an identifier that identifies the corresponding encrypted packet, storing management information to show a correspondence between the encrypted packet and the PID thereof would be irrelevant in Candelore et al.

Therefore, it is respectfully submitted that Candelore et al does not disclose or suggest the feature of the present invention as recited in independent claims 8 and 20 whereby the encryption key data and the encrypted data are stored, and management information showing correspondence between the encryption key data and the encrypted data, both of which have been acquired from the same compressed data is also stored, and the stored

encryption key data and the stored encrypted data, both of which have been acquired from the same compressed data are extracted based on the stored management information, and then the extracted encryption key data and the extracted encrypted data are combined and decoded back to the compressed data.

Yet still further, with respect to claim 13, Candelore et al teaches that when a program with encrypted content is received, the encrypted packets are decrypted based on their PIDs. However, Candelore et al does not disclose or suggest that, for a given packet, the PID of the packet and specific information which identifies the encrypted packet corresponding to the PID is output in a predetermined form to an external user as according to claim 13 of the present invention.

Therefore, it is respectfully submitted that Candelore et al does not disclose or suggest the feature of the present invention as recited in independent claim 13 whereby the encryption key data and specific information which identifies stored encrypted data corresponding to the encryption key data is output in a predetermined form to an external user.

In view of the foregoing, it is respectfully submitted that the present invention as recited in independent claims 7, 8, 13 and 20 and claims 9-12 and 14-19 respectively depending therefrom, all clearly patentably distinguish over Candelore et al, under 35 USC 102 as well as under 35 USC 103.

Allowance of the claims and the passing of this application to issue are respectfully solicited.

If the Examiner has any comments, questions, objections or recommendations, the Examiner is invited to telephone the undersigned at the telephone number given below for prompt action.

Respectfully submitted,

/Douglas Holtz/

Douglas Holtz
Reg. No. 33,902

Frishauf, Holtz, Goodman & Chick, P.C.
220 Fifth Avenue - 16th Floor
New York, New York 10001-7708
Tel. No. (212) 319-4900
Fax No. (212) 319-5101

DH:jd